93RD DISTRICT
STATE CAPITOL
P.O. BOX 30014
LANSING, MI 48909-7514
PHONE: (517) 373-1778
FAX: (517) 373-5780
E-MAIL: paulopsommer@house.mi.gov

MICHIGAN HOUSE OF REPRESENTATIVES

PAUL E. OPSOMMER

STATE REPRESENTATIVE

March 26, 2009

Chairperson Pamela Byrnes
Honorable members of the Michigan House Transportation Committee

Last year Michigan rushed into legislation that allowed for the creation of an Enhanced Drivers License program. While we tried to put protections into that bill for data to be encrypted, and for data not to be shared with Mexico and Canada, now that we have seen the formal agreement that the federal government would like us to enter into, it is apparent that those safeguards have been ignored. The data would not be encrypted, and details on foreign data sharing are still murky. We are moving too fast on this with too many unanswered questions.

Just this week, the government in Saskatchewan scrapped their EDL plans, even after already spending $600,000 on the project. The concerns listed in various articles included cost, continually changing requirements, and privacy concerns. In February, British Columbia took back an EDL database it had given to the United States over data sharing concerns.

If the Canadians are concerned about how all this will work with the United States and Mexico, we need to be as well. The National Conference of State Legislator in December of last year voted unanimously on a resolution urging the federal government to allow States to make their own technology decisions. I feel strongly that Michigan should join in that fight with HCR 006 and HR 11, as the safeguards are not there.

Let me be clear, the RFID that would be put into EDLs is different than the RFID that is put into traditional passports. Traditional passports use short range transmission, encryption, and basic access control. The EDLs instead use long range unencrypted technology. The only protection they offer are twofold: 1) they will be issued in a metallic sleeve to shield the data, and 2) it will only transmit a new unique personal identifier, and not a name. The sleeve obviously is compromised every time the license is taken out, whether at the border, the bank, or a big box store. It can then be read both instantly and silently by anyone within 20-30 feet range. The personal identifier, which is in essence a new social security number for citizens, will be piggybacked upon and used by others for their own purpose. While most people who get that number will not be able to hack the EDL database, they will be able to associate that new unique ID number with a name and person, and create new and separate databases to track them.

MEMORANDUM OF AGREEMENT BETWEEN THE STATE OF MICHIGAN & DEPARTMENT OF HOMELAND SECURITY

I. PARTIES

The Parties to this Memorandum of Agreement (hereinafter "MOA") are the State of Michigan, hereinafter referred to as "State of Michigan," and the Department of Homeland Security, hereinafter referred to as "DHS" (collectively, the "Parties").

II. AUTHORITY

DHS is authorized to enter into this MOA pursuant to the Homeland Security Act of 2002, 6 U.S.C. § 112(b), as amended. The State of Michigan is authorized to enter into this MOA pursuant to Michigan state statute 2008 PA 23.

III. ENHANCED DRIVER'S LICENSE

A. PURPOSE

This MOA demonstrates the Parties' shared commitment to support the State of Michigan's enhanced driver's license voluntary project. Under the voluntary project, the State of Michigan and DHS will develop, issue and accept a valid and lawfully obtained enhanced driver's license and identification card with facilitative technology for border crossing purposes. The Secretary of Homeland Security expects that a valid and lawfully obtained State of Michigan enhanced driver's license, or identification card for those who do not drive, be accepted as an alternative Western Hemisphere Travel Initiative (WHTI) document for land and sea border crossings.

The Secretary of Homeland Security also expects the requirements for the enhanced driver's license to align and be consistent with the minimum document requirements and issuance standards detailed in the REAL ID regulation.

The documents issued by the State of Michigan as an enhanced driver license or identification card will be collectively referred to in this MOA as the "Enhanced Driver's License".

B. BACKGROUND

The tragic aftermath of the September 11, 2001 terrorist attacks required thoughtful and immediate improvements to our nation's border security. WHTI implements a Congressional requirement that all United States citizens and other travelers to and from Canada, Mexico, Central and South America, the Caribbean and Bermuda present a passport or other accepted

document that establishes the bearer's identity and citizenship to enter or re-enter the United States. The goal is to strengthen border security and facilitate entry into the United States for U.S. citizens and legitimate international travelers. It is anticipated that the date of full WHTI implementation will be in the summer of 2009 when U.S. citizens traveling between the U.S. and Canada, Mexico, Central and South America, the Caribbean, and Bermuda by land or sea (including ferries), will be required to present a valid U.S. passport or other document acceptable to the Secretary of Homeland Security.

The Parties anticipate that a valid and lawfully obtained Enhanced Driver's License issued by the State of Michigan will be an acceptable alternative document for U.S. citizens. Such an enhanced document would advance the security and economic interests of the region's citizens.

The driver's license is a nationally accepted means of identification. A driver's license can be enhanced to securely denote identity and citizenship. The holder of a valid and lawfully obtained Enhanced Driver's License will then also be able to use that document to show citizenship and identity at a significant cost savings to the applicant.

A successful project will also serve the mutual interests of DHS and the State of Michigan by increasing the use of facilitative technology, thereby facilitating cross border trade and travel, and providing another secure document option to U.S. citizens residing in Michigan that can meet the security goals of WHTI.

C. PROJECT RESPONSIBILITIES

The State of Michigan shall be responsible for:

(1) Making the necessary investments in technology, process changes and resources to accommodate the requirements of Enhanced Driver's Licenses.

(2) Making any legislative, regulatory or policy/procedure changes to facilitate the implementation of the requirements of Enhanced Driver's Licenses.

(3) Ensuring that systems, programs and safeguards are in place that protect an individual's Personally Identifiable Information (PII).

(4) Issuing an Enhanced Driver's License that denotes, pursuant to issuance standards established by DHS and provided for in the business plan, the identity and U.S. citizenship of State of Michigan residents.

(5) Including facilitative technology identified by DHS in the Enhanced Driver's License that will facilitate identity and citizenship validation through the sharing of information and include the current status of the card holder's right to use the Enhanced Driver's License.

(6) Developing a business plan for the voluntary project, in conjunction with DHS that addresses and implements minimum business requirements that are acceptable to

DHS, including technology requirements, document requirements (data elements and physical security features on the driver's license and identification cards), issuance requirements, employee background checks, training, security and confidentiality of information and records collected and maintained by the DMV, verification of information presented on source documents, and database connectivity,

(7) Allowing DHS to review the operations of the project and responding to any comments from DHS.

(8) Ensuring that employees involved in the project have undergone background checks acceptable to DHS.

(9) Committing to compliance with the REAL ID milestones put forth in the REAL ID regulation.

The Department of Homeland Security shall be responsible for:

(1) Accepting for border crossing purposes under WHTI, pending implementation of regulations on acceptable documents, the State of Michigan's denotation of identity and citizenship on the Enhanced Driver's License

(2) As long as the state is compliant with REAL ID milestones, as put forth in the regulation, accepting for official purposes, as defined by the REAL ID Act and REAL ID rulemaking process, the State of Michigan's Enhanced Driver's License.

(3) Providing the facilitative technology specifications for the Enhanced Driver's License, providing the facilitative technical specifications for an interactive validation process and utilizing these facilitative technologies.

(4) Establishing minimum standards for the project including issuance standards for the Enhanced Driver's License.

(5) Approving a detailed State of Michigan business plan for the project that implements minimum business requirements acceptable to DHS.

(6) Reviewing the operation of the project pursuant to the business plan and providing comments to the State of Michigan.

(7) Providing any additional assistance as determined by DHS to be necessary for successful implementation of the Enhanced Driver's License Project.

(8) Supporting the development of the verification hub.

IV. POINTS OF CONTACT

FOR DHS:
Adina Kazyak Ordonez
Screening Coordination Office

FOR the State of Michigan:
Brian DeBano
Chief of Staff / Chief Operating Officer
Michigan Department of State

V. TERM AND TERMINATION

Either Party may terminate this MOA upon the giving of written notice thirty (30) calendar days in advance of the termination date to the other Party.

VI. MODIFICATION

Modifications to the MOA may be made only by mutual consent of the Parties, in the form of a written modification, signed and dated by both Parties, with the approval of the State Administrative Board.

VII. FUNDING

This MOA does not obligate DHS funds and is not intended to provide any funding or financial support for the State of Michigan Enhanced Driver's License project.

VIII. EFFECTIVE DATE

The parties agree that this MOA is effective upon enactment.

IX. CONFIDENTIALITY

Each Party understands that the other Party or third parties may disclose to it information designated by another party as confidential information related to the project discussed in this MOA.

Each Party agrees to maintain in confidence such information and to use this information solely to provide services related to the project under this MOA. Except as required by law, each Party shall not disclose this information to any person except authorized contractors who also agree not to disclose this confidential information. Each Party shall include requirements of confidentiality for any person that has access to the confidential information pursuant to this MOA.

Each Party shall take reasonable measures to maintain the confidentiality of this information pursuant to the business plan. Each Party shall give prompt notice to the other Party of any request for, use of, or disclosure of confidential information and agrees to assist the other in responding to any request, remedying any misuse, or remedying any inappropriate disclosure.

Further, DHS agrees that all materials containing confidential information received pursuant to this MOA concerning State of Michigan residents and its employees, and any other information that may be considered confidential, shall not be disclosed to other persons without the State of Michigan's written consent, except as may be required by law. Any personal information received by DHS shall be handled by DHS, as appropriate and necessary, in accordance with the Privacy Act of 1974, as amended.

X. MISCELLANEOUS

This MOA does not confer a right or benefit on behalf of any third party and does not otherwise confer a right on any third party to enforce a term of this MOA.

This MOA represents the entire agreement between the Parties. No other understanding, oral or otherwise, regarding the subject matter of this MOA shall be deemed to exist or to bind any of the parties hereto.

IN WITNESS WHEREOF, the Parties have signed two (2) duplicate originals of this MOA.

Department of Homeland Security	**State of Michigan**
_____	_____
(Signature) *(Date)*	*(Signature)* *(Date)*
Michael Chertoff	Terri Lynn Land
(Print Name)	*(Print Name)*
Secretary, Department of Homeland Security	Michigan Secretary of State
(Title)	*(Title)*

Saskatchewan scraps plan to offer enhanced driver's licences

BY ANGELA HALL, LEADER-POST MARCH 23, 2009

REGINA -- After spending more than $600,000 pursuing the idea, the Saskatchewan Party government is officially scrapping a plan to offer enhanced driver's licences that could've been used in place of a passport when driving to the U.S.

Crown Corporations Minister Ken Cheveldayoff said the project grew less attractive as the estimated per-licence cost grew higher.

SGI will instead launch a campaign encouraging residents to get a passport if they want to prevent getting stuck at the border, the minister told reporters.

Under the Western Hemisphere Travel Initiative, Canadians wishing to travel to the U.S. as of June 2009 will require a passport or other secure identification to cross the border by land. A passport is already required for travel by air.

"I was comfortable in the $25 to $50 range, but when I saw those costs (for an enhanced driver's licence) go above $50 and nearing the cost of getting a passport, the argument for just having a passport became stronger and stronger and I think logically we've made the right decision here," Cheveldayoff said.

He defended the $600,000 expenditure made by SGI as a "very modest amount" in the context of the Crown corporation's overall budget. The business may recoup some of that money, as a portion went toward leasing additional office space in Saskatoon that may now be sublet.

Privacy concerns about the enhanced licences also factored into the government's decision, Cheveldayoff said.

Earlier this month, Information and Privacy Commissioner Gary Dickson raised his objections with legislation the government had proposed to allow for the introduction of the licences. Dickson said the bill wasn't clear on the risks to privacy associated with the radio frequency identification tags that would be part of the licences, among other concerns.

"I think this is an excellent move on the part of our provincial government," Dickson said Monday.

"My expectation now is that some of those other provinces that were going down the road of an enhanced driver's licence may in fact now have reason to pause and rethink that."

Alberta decided not to pursue the enhanced licences at all, while B.C., Manitoba, and Ontario are

among the jurisdictions that expect to offer them.

NDP MLA Pat Atkinson questioned whether the brakes would have been put on the Saskatchewan plan if the Opposition hadn't raised the privacy concerns in the legislature. The government might not have needed to spend $600,000 pursuing the plan if there had been more discussions about the concept earlier on, she said.

ahall@leaderpost.canwest.com

NCSL Policy Statement:

The Western Hemisphere Travel Initiative (WHTI)

Adopted 2008

On April 5, 2005, the Departments of Homeland Security and State announced the Western Hemisphere Travel Initiative (WHTI), which would require all travelers to and from the United States to have a passport (or other approved documents) to enter or re-enter the United States. The federal government asserts that this initiative will increase the safety measures at the borders. WHTI was based on the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTP).

On September 1, 2005, the U.S. government published in the Federal Register an Advanced Notice of Proposed Rulemaking (ANPR) on the plan to implement the WHTI, and set proposed implementation dates, stating that the rules will apply to all individuals traveling to the United States by air and by sea beginning December 31, 2006, and would apply to all individuals entering or re-entering the U.S. via its land border crossings as of December 31, 2007. However, subsequent federal legislation delayed full implementation for WHTI land border crossing requirements until June of 2009 or later. The Final Rules for WHTI were subsequently published in April of 2008. In addition to focusing on citizenship and identity as required by the IRTP of 2004, it would appear that the Final Rules also call for the use of RFID technology for travel documents to meet DHS approval.

Impacts on Trade and Tourism

The WHTI will be a deterrent to travel and negatively impact the total number of border crossings, having significant implications for the economies of the United States, Canada, and Mexico.

The Canada–United States border relationship has more than 300,000 business people, tourists, and regular commuters traveling between Canada and the United States every day. On average $1.1-billion in goods crosses the Canada-United States Border every day. It is estimated that fifty-six percent (56%) of same-day travelers from the United States, forty percent (40%) of same-day travelers from Canada, fifty percent (50%) of overnight travelers from the United States, and thirty percent (30%) of overnight travelers from Canada do not possess a passport, primarily due to cost.

A recent report prepared by Conference Board of Canada for the Canadian Tourism Commission estimates that this passport requirement would result in 3.5 million fewer trips into the United States from Canada by 2008 with a related loss of $785 million in potential tourism revenue. Likewise, the report estimates 7.7 million fewer trips by U.S. citizens into Canada and $1.7 billion in lost revenues.

NCSL also acknowledges the importance of the cultural, economic and trade issues unique to the border between the United States and Mexico, and hereby expresses concern about the potential economic impact of the WHTI policy on the states which border Mexico.

Core Solutions and Alternative Measures to the WHTI

NCSL applauds efforts by the U.S. Departments of Homeland Security and State to further secure America's borders and protect the well-being of U.S. residents and their property. However, NCSL strongly encourages the federal government to do so in a manner that addresses the root problems associated with an increased usage of passport documents, the core intent of the IRTP, and the sovereignty of state documents.

In addition, NCSL also encourages the federal government to fully explore federal frequent border-crossing programs – such as NEXUS, FAST, CANPASS and other proposed federal passport substitutes – that recognize the benefits of the trade and tourism traffic that economically helps the people and nations on both sides of the border.

This is particularly important given the high price of traditional passports, whose prices have more than doubled over the past 10 years and now cost more than $100. While these alternatives represent important options under WHTI, they also carry limitations.

An example is the new PASSport Card, a 'passport lite' federal identity document that is considerably less expensive at $45. It is of limited utility however in that it is only approved for ground border crossings, and not air travel. It also incorporates the use of RFID technology in a manner different than traditional passports that some have found controversial. How much the card will be get used, and thus help to alleviate WHTI border concerns, is debatable. NCSL therefore asserts that it would be preferential to instead make fully utilizable traditional passports available at a lower end cost to taxpayers, a document that can be used for both air and ground travel, and that employs more traditional RFID technology. NCSL therefore supports the US Congress

implementing a fully refundable federal income tax credit, that allows for a credit equal to 50% of the price of a passport, to reduce its end cost to consumers to a price level similar to the proposed Passport Cards.

Likewise, another alternative presented under WHTI by DHS is the creation of Enhanced Drivers Licenses (EDLs), which merge state driver's licenses with federal procedures and RFID technology to create a DHS approved WHTI travel document. These cards have been controversial as they affect the sovereignty of a state document, creating a new hybrid or an unknown legal nature, and have met with resistance in some states because the DHS has mandated that the cards must use unencrypted, long range vicinity read RFID technology. In consideration of the fact that the WHTI as passed by Congress only mandates proof of identity and citizenship, and not technology, it is the policy of NCSL to work with Congress and the DHS to develop an acceptable EDL that has its core requirements concerns over matters of identity and citizenship, and that is not predicated on states having to accept the use of RFID or other remote technology in their driver's licenses. This is particularly important considering that many other RFID enabled document options already exist, and would give states and their citizens' flexibility that respects their sovereignty and desire for alternatives that do not compromise identity or proof of citizenship.

Conclusion

The NCSL implores the federal government – the U.S. Congress, the President, and the U.S. Departments of Homeland Security and State – to fully and effectively consult with NCSL and state legislatures to ensure that these and other state interests and concerns are factored into the WHTI and other border security programs. Programs that are not acceptable to the states or its citizens will ultimately not be extensively employed or used, compounding the negative economic impacts of the WHTI. The NCSL also asks for Congressional oversight over the implementation of the WHTI program, to make sure that it meets the core needs of identity and proof of citizenship, while not mandating a one size fits all approach to technology, biometrics, or other mandates that force the states to evaluate their participation in the program in a cookie cutter manner outside of the original intent of the WHTI.

NCSL also advocates and supports the US Congress implementing a fully refundable federal income tax credit, that allows for a credit equal to 50% of the price of a passport,

to reduce its end cost to consumers to a price level similar to the proposed Passport Cards.

NCSL looks forward to working with the appropriate federal officials as they work to guarantee American security while sustaining American freedoms, quality of life and commerce.

August 2011

NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

NCSL OPPOSES FEDERAL TECHNOLOGY MANDATES FOR STATE ISSUES IDENTIFICATION DOCUMENTS

NCSL STANDING COMMITTEE ON COMMUNICATIONS, FINANCIAL SERVICES & INTERSTATE COMMERCE

WHEREAS, the federal government is taking a more active role in influencing and determining the technological standards for state issued identification documents such as drivers licenses. The federal government is attempting to influence or mandate the technological standards of sovereign state issued identification documents through the direct acts of Congress, the rule-making processes of the Departments of State and Homeland Security, or through both official or informal agreements with international organizations or initiatives such as the American Association of Motor Vehicle Administrators (AAMVA), the Security and Prosperity Partnership (SPP), and the United Nation's agency known as the International Civil Aviation Organization (ICAO).

WHEREAS, an example contrary to the tenets of federalism, the initial version of the federal REAL ID Act as introduced would have required the states to enter into the AAMVA compact known as the Driver's License Agreement (DLA). This compact as drafted would put the non-governmental 501c3 AAMVA, which has foreign voting members, in charge of making the technology decisions for a state's sovereign drivers licenses. Such federal decisions would allow for AAMVA, and not the States, to determine whether or not particular technology must be employed, whether or not such data could be encrypted, what biometrics would need to be encoded, and whether or not the data could be shared with foreign governments.

WHEREAS, an example contrary to the tenets of federalism, the final rules for both REAL ID and the Western Hemisphere Travel Initiative (WHTI) were published in 2008, and mandated standards onto states' driver's licenses for them to be acceptable for certain uses. The Department of Homeland Security is currently requiring states to embed unencrypted contactless technology into a state's drivers licenses in order for citizens to be able to use them to get back into the United States at international ground crossings. This places specific technological choices as having equal importance over the roles of identification and proof of citizenship, while leaving states with no flexibility or options in this

area if they want to pursue an Enhanced Drivers License (EDL) that does not use technology, wish to employ encrypted technology, or wish to employ shorter range technology than what is being mandated. The goal of WHTI deals simply with providing proof of citizenship, not dictating the technology by which that proof must be conveyed.

WHEREAS, an example contrary to the tenets of federalism, the final rules for REAL ID, page 86, make clear that the federal government is not satisfied with a one time mandate and wishes to have this control in perpetuity going forward: "Moreover, in the future, DHS, in consultation with the States and DOT, may consider technology alternatives to the PDF417 2D bar code that provide greater privacy protections after providing for public comment". The "final rules" are therefore not really final, and it is unacceptable that such technological decisions could be made by requiring only non-binding consultation with States, especially when there is debate between the States and the federal government as to what really constitutes optimal privacy and security options for their driver's licenses.

WHEREAS, a driver's license is a sovereign state document, and whether or not particular technology must be employed, should remain a State decision. The federal government should not use the WHTI, a policy of its own devising, as an economic cudgel to coerce states into accepting such technological standards onto their sovereign driver's licenses.

THEREFORE, let it be resolved, that the NCSL will urge the President, Congress, and the Departments of State, Transportation, and Homeland Security to not pass law, allow for federal policy, to use international organizations, or to enter into international agreements that mandate or attempt to indirectly influence the use of particular technology in state or local identity documents.

Adopted by the NCSL Communications, Financial Services and Interstate Commerce Committee, December 12, 2008.

Unanimously passed the full NCSL Business Meeting, December 13, 2008.

Canada

David Loukidelis, B.C.'s information and privacy commissioner.

Ottawa recalls sensitive database in border project

Updated Sun. Feb. 15 2009 2:26 PM ET

The Canadian Press

OTTAWA -- The federal government is repatriating a database of personal information about Canadian citizens after warnings the U.S. government might misuse it.

The database with details about several hundred British Columbians was turned over to the U.S. Customs and Border Protection agency last year as part of a controversial project to issue "enhanced driver's licences" instead of passports for land-border crossings.

The pilot project is the first step in a Canada-wide program that could have seen the personal information of hundreds of thousands of Canadians handed over wholesale to American officials.

But the Canada Border Services Agency has bowed to pressure from privacy advocates and is recalling the database, with the U.S. border agency promising to erase its records.

Instead, as the project expands, the growing personal databanks will reside in Canada, accessible electronically -- with strict limits -- by American border officials.

"The data will remain in Canada, and it will be accessed remotely," said David Loukidelis, British Columbia's privacy commissioner and a critic of the original plan.

Washington has been toughening rules for people entering the United States from Canada, requiring passports for air passengers in 2007 and, as of June 1 this year, passports for travellers by land and water.

However, American officials will also accept so-called "enhanced driver's licences" at land and marine border points in lieu of a passport, through a joint program developed with Ottawa.

The B.C. pilot project signed up 521 citizens in that province as volunteers, and issued each of them a special driver's licence with an embedded chip, known as a radio-frequency identification device or RFID.

The chips, which can be read by electronic scanners up to 4.5 metres away, contain a unique identifying number for each card holder. During the pilot project, American border officials scanned the RFID and used the unique number to locate the personal information of the bearer in the database supplied by Canada.

The personal data included full name, birth date, gender, citizenship and other information that is ordinarily also contained in a passport. In addition, U.S. officials could access a digital image of the bearer.

The Canada Border Services Agency signed an agreement with its American counterpart to ensure that the information would be accessed only by U.S. officers at the time of crossing for border purposes only.

However, the USA Patriot Act could trump that clause, forcing the U.S. border service to turn over information to American security agencies.

"It is clear that there is potential for secondary use," says a federal-provincial review of the project, dated Aug. 14 and obtained under the Access to Information Act.

"Further, it is possible that if there was disclosure pursuant to the USA Patriot Act that CBP (U.S. Customs and Border Protection) may not be legally able to advise CBSA."

The review also expressed concern that the digital image, which is not currently contained in Canadian passports, "does have the potential to be used for secondary purposes as a biometric identifier."

Volunteer participants in the B.C. project were warned their personal

RELATED STORIES

- Border agency misses target on firearm records: audit
- Officials unclear on extent of gun smuggling
- Border agency to expand surveillance program
- Canada, Greece have best privacy records: report

USER TOOLS

del.icio.us | DIGG
Share on Twitter | Facebook
Print This Page | E-Mail Story
Feedback | Fonts: **Bigger** **Smaller**

CANADIAN STORIES

- Hundreds on flood evacuation alert in Manitoba
- Quebec police arrest 11 allegedly linked to gangs
- Rescuers hope to resume search for snowmobilers
- CAW and Chrysler hope to reach deal today
- Jewish group proud of role in barring Galloway
- Ontario to help offset harmonized PST: CTV
- Budget officer forecasts major decline in GDP
- War resister gets 11th-hour stay from deportation
- Officials want Snowbirds to use aging planes to 2020
- RIM shares slide on U.S. analyst's warning
- Livent co-founders found guilty of fraud, forgery

information could be disclosed beyond the American border service "to other organizations for any other purpose as authorized by U.S. law."

Still, a survey last year showed that 14 per cent of informed participants remained concerned about where that information might end up.

A spokeswoman for U.S. Customs and Border Protection confirmed the agency plans to return the pilot database to Canada.

"Phase 1 data currently resides in a secure CBP database and will be transitioned to a CBSA database," said Joanne Ferreira from Washington, D.C.

"CBP will delete Phase 1 records from the CBP database -- co-ordinated with CBSA -- so there will be no overlap."

Each time personal data is accessed at the border, however, it is recorded permanently in the U.S. Treasury Enforcement Communications System or TECS, just as similar information is recorded in TECS whenever a passport holder is checked at the Canada-U.S. border.

The second phase of the B.C. project, open to all Canadian citizens living in the province, is set to be launched this spring for those who don't want to use a passport.

About 48,000 of the enhanced driver's licences are expected to be issued, said Alex Dabrowski, a spokesman for the British Columbia government in Victoria. The fee has not yet been established.

Saskatchewan, Manitoba, Ontario, Quebec and Nova Scotia have also asked to sign on, some as early as this spring.

In the meantime, privacy advocates remain concerned about the RFID technology, for fear the chips could be used to secretly track Canadian citizens. Ferreira says RFID scanners have been installed only at the Peace Arch and Pacific Highway points of entry in Washington State.

"It's an insecure technology," said Loukidelis. "It could be used theoretically to track people, and I think that's something we want to try and avoid."

There are also fears the information could be "skimmed" by hackers to help steal identities, although the card itself does not contain personal data.

As an interim step, users are provided so-called Faraday sleeves that slip over the card and block scanners from reading the RFID chip.

USER TOOLS

del.icio.us
DIGG
Share on Twitter
Facebook
Print This Page
E-Mail Story
Feedback

CANADIAN STORIES

- Hundreds on flood evacuation alert in Manitoba
- Quebec police arrest 11 allegedly linked to gangs
- Rescuers hope to resume search for snowmobilers
- CAW and Chrysler hope to reach deal today
- Jewish group proud of role in barring Galloway
- Ontario to help offset harmonized PST: CTV
- Budget officer forecasts major decline in GDP
- War resister gets 11th-hour stay from deportation
- Officials want Snowbirds to use aging planes to 2020
- RIM shares slide on U.S. analyst's warning
- Livent co-founders found guilty of fraud, forgery

About CTV| Contests | Careers | CTV Announcements | Advertise on TV | CTV Media | Advertise on Web
Archive Sales | Tapes and Transcripts | Privacy Policy | Terms and Conditions | Contact Us | Site Map

- **Blog Home**

Search Find

Next: Women's Suffrage Abandoned. "Too Unpopular," says Anthony.

Previous: Slashed?

EDLs on the Ropes

Posted by Jim Harper

With the REAL ID Act floundering in state resistance, DHS officials and government contractors have been pinning their hopes on "enhanced drivers licenses" or EDLs. These are state-issued driver's licenses that the Department of Homeland Security and State Department have agreed to treat as proof of citizenship for purposes of border crossings.

With the flexibility of doing things by fiat, outside of a statutory process, the bureaucracy had gotten some traction with this ID system — most notable for its use of long-range RFID (radio frequency identification tags) to track people.

But news comes today that the Canadian province of Saskatchewan is scrapping its plans to create EDLs for U.S. border crossings, mostly due to cost.

> "I was comfortable in the $25 to $50 range, but when I saw those costs (for an enhanced driver's licence) go above $50 and nearing the cost of getting a passport, the argument for just having a passport became stronger and stronger and I think logically we've made the right decision here," [Crown Corporations Minister Ken] Cheveldayoff said.

With more vocal opposition to RFID-based tracking in EDLs south of the border (that is, here in the states), the U.S. EDL may run into more than just cost concerns. And there is discomfort brewing with federal agencies cooking up an identity system on their own.

For all its faults, at least REAL ID had a statutory mandate. EDLs could end up being anything bureaucrats want them to be, which could be worse than what Congress put together in REAL ID.

Jim Harper • March 25, 2009 @ 8:30 am
Filed under: Foreign Policy and National Security; Telecom, Internet & Information Policy; Trade
Tags: border crossings, department of homeland security, drivers licenses, proof of citizenship, real id act

ShareThis

Related Posts

- DHS Officials Skirt Open Meeting Laws to Promote REAL ID
- Awesome, Fearsome, Awesome - Or Maybe Silly
- National-ID-Backing Intel Chief Steps Down

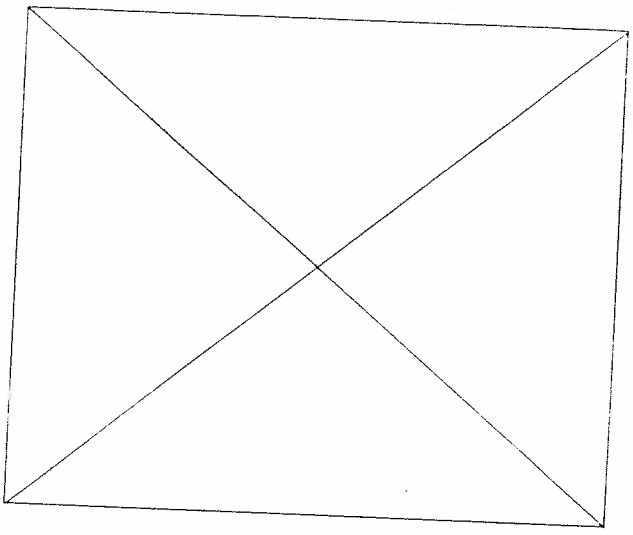
SCIENTIFIC AMERICAN

Scientific American Magazine - August 21, 2008

How RFID Tags Could Be Used to Track Unsuspecting People

A privacy activist argues that the devices pose new security risks to those who carry them, often unwittingly

By Katherine Albrecht



If you live in a state bordering Canada or Mexico, you may soon be given an opportunity to carry a very high tech item: a remotely readable driver's license. Designed to identify U.S. citizens as they approach the nation's borders, the cards are being promoted by the Department of Homeland Security as a way to save time and simplify border crossings. But if you care about your safety and privacy as much as convenience, you might want to think twice before signing up.

The new licenses come equipped with radio-frequency identification (RFID) tags that can be read right through a wallet, pocket or purse from as far away as 30 feet. Each tag incorporates a tiny microchip encoded with a unique identification number. As the bearer approaches a border station, radio energy broadcast by a reader device is picked up by an antenna connected to the chip, causing it to emit the ID number. By the time the license holder reaches the border agent, the number has already been fed into a Homeland Security database, and the traveler's photograph and other details are displayed on the agent's screen.

Although such "enhanced" driver's licenses remain voluntary in the states that offer them, privacy and security experts are concerned that those who sign up for the cards are unaware of the risk: anyone with a readily available reader device—unscrupulous marketers, government agents, stalkers, thieves and just plain snoops—can also access the data on the licenses to remotely track people without their knowledge or consent. What is more, once the tag's ID number is associated with an individual's identity—for example, when the person carrying the license makes a credit-card transaction—the radio tag becomes a proxy for that individual. And the driver's licenses are just the latest addition to a growing array of "tagged" items that consumers might be wearing or carrying around, such as transit and toll passes, office key cards, school IDs, "contactless" credit cards, clothing, phones and even groceries.

RFID tags have been likened to barcodes that broadcast their information, and the comparison is apt in the sense that the tiny devices have been used mainly for identifying parts and inventory, including cattle, as they make their way through supply chains. Instead of having to scan every individual item's Universal Product Code (UPC), a warehouse worker can register the contents of an entire pallet of, say, paper towels by scanning the unique serial number encoded in the attached RFID tag. That number is associated in a central database with a detailed list of the pallet's contents. But people are not paper products. During the past decade a shift toward embedding chips in individual consumer goods and, now, official identity documents has created a new set of privacy and security problems precisely because RFID is such a powerful tracking technology. Very little security is built into the tags themselves, and existing laws offer people scant protection from being surreptitiously tracked and profiled while living an increasingly tagged life.

Beyond Barcodes

The first radio tags identified military aircraft as friend or foe during World War II, but it was not until the late

1980s that similar tags became the basis of electronic toll-collection systems, such as E-ZPass along the East Coast. And in 1999 corporations began considering the tags' potential for tracking millions of individual objects. In that year Procter & Gamble and Gillette (which have since merged to become the world's largest consumer-product manufacturing company) formed a consortium with Massachusetts Institute of Technology engineers, called the Auto-ID Center, to develop RFID tags that would be small, efficient and cheap enough to eventually replace the UPC barcode on everyday consumer products.

By 2003 the group had developed a working version of the technology and attracted investment from more than 100 companies and government agencies. The tags' promoters promised the tiny chips would revolutionize inventory management and counterfeiting prevention [see "RFID: A Key to Automating Everything," by Roy Want; Scientific American, January 2004].

To kick-start government adoption of the technology, the General Services Administration (GSA), a federal bureau that manages purchasing for other government institutions, issued a memo in 2004 urging the heads of all federal agencies "to consider action that can be taken to advance the [RFID] industry." Suddenly, virtually every agency, from the Social Security Administration to the Food and Drug Administration, began announcing RFID trials.

During the same period, similar initiatives were under way around the world. In 2003 the International Civil Aviation Organization (ICAO), a United Nations agency that sets global passport standards, endorsed the use of RFID tags in passports. ICAO now calls for their use in all scannable "e-passports." Today dozens of countries, including the U.S., issue e-passports with RFID tags embedded in their covers.

Since their debut, the new passports have been controversial on both privacy and security grounds. In a 2006 report one ICAO official promised that encryption measures would provide a "level of protection [that] should reassure the most anxious passport holder that his personal data cannot be read without his knowledge."

Security experts quickly proved otherwise. In 2007 British security consultant Adam Laurie cracked the encryption code on a U.K. passport and "skimmed," or remotely read, its personal information—while it was still sealed in its mailing envelope. Around the same time, German security consultant Lukas Grunwald copied the data from a German passport's embedded chip and encoded it into a different RFID tag to create a forged document that could fool an electronic passport reader. Investigators at Charles University in Prague, finding similar vulnerabilities in Czech e-passports, wrote that it was "a bit surprising to meet an implementation that actually encourages rather than eliminates [security] attacks."

Yet these demonstrated security problems have not slowed the adoption of RFID. On the contrary, the technology is being deployed for domestic ID cards around the world. Malaysia has issued some 25 million contactless national identity cards. Qatar is issuing one that stores the cardholder's fingerprint in addition to personal information. And in what industry observers are calling the single largest RFID project in the world, the Chinese government is spending $6 billion to roll out RFID-based national IDs to nearly one billion citizens and residents.

There is an important difference, however, between other nations' RFID-based ID cards and Homeland Security's new driver's licenses. Most countries' contactless national IDs and e-passports have adopted an RFID tag that meets an industry standard known as ISO 14443, which was developed specifically for identification and payment cards and has a degree of security and privacy protection built in. In contrast, U.S. border cards use an RFID standard known as EPCglobal Gen 2, a technology that was designed to track products in warehouses, where the goal is not security but maximum ease of readability.

Whereas the ISO 14443 standard includes rudimentary encryption and requires tags to be close to a scanner to be read (a distance measured in inches rather than feet), Gen 2 tags typically have no encryption and only minimal data safeguards. To skim the data from an encrypted ISO 14443 chip, you have to crack the encryption code, but no special skills are required to skim a Gen 2 tag; all you need is any Gen 2 reader. Such readers can be purchased readily and are in common use in warehouses worldwide. A hacker or criminal armed with one could skim a border card through a purse, across a room, even through a wall.

As of this past April, more than 35,000 Washington State motorists had signed up for enhanced driver's licenses, and other border states, including Arizona, Michigan and Vermont, have agreed to participate in the

program. New York State will begin making the new licenses available to its residents after Labor Day.

But the possibility that the security of such cards could be compromised is just one reason for concern. Even if tighter data-protection measures could someday prevent unauthorized access to RFID-card data, many privacy advocates worry that remotely readable identity documents could be abused by governments that wish to tightly monitor and control their citizens.

China's national ID cards, for instance, are encoded with what most people would consider a shocking amount of personal information, including health and reproductive history, employment status, religion, ethnicity and even the name and phone number of each cardholder's landlord. More ominous still, the cards are part of a larger project to blanket Chinese cities with state-of-the-art surveillance technologies. Michael Lin, a vice president for China Public Security Technology, a private company providing the RFID cards for the program, unflinchingly described them to the New York Times as "a way for the government to control the population in the future." And even if other governments do not take advantage of the surveillance potential inherent in the new ID cards, ample evidence suggests that data-hungry corporations will.

Living a Tagged Life

If the idea that corporations might want to use RFID tags to spy on individuals sounds far-fetched, it is worth considering an IBM patent filed in 2001 and granted in 2006. The patent describes exactly how the cards can be used for tracking and profiling even if access to official databases is unavailable or strictly limited. Entitled "Identification and Tracking of Persons Using RFID-Tagged Items in Store Environments," it chillingly details RFID's potential for surveillance in a world where networked RFID readers called "person tracking units" would be incorporated virtually everywhere people go—in "shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums"—to closely monitor people's movements.

According to the patent, here is how it would work in a retail environment: an "RFID tag scanner located [in the desired tracking location]... scans the RFID tags on [a] person.... As that person moves around the store, different RFID tag scanners located throughout the store can pick up radio signals from the RFID tags carried on that person and the movement of that person is tracked based on these detections.... The person tracking unit may keep records of different locations where the person has visited, as well as the visitation times."

The fact that no personal data are stored in the RFID tag does not present a problem, IBM explains, because "the personal information will be obtained when the person uses his or her credit card, bank card, shopper card or the like." The link between the unique RFID number of the tag and a person's identity needs to be made only once for the card to serve as a proxy for the person thereafter. Although IBM envisioned tracking people via miniature tags in consumer goods, with today's RFID border cards there is no need to wait for such individual product tags to become widespread. Washington's new driver's licenses would be ideally suited to the in-store tracking application, because they can already be read by Gen 2 inventory scanners in use today at stores such as Wal-Mart, Dillard's and American Apparel.

A tracking infrastructure will become increasingly fruitful to marketers as more people begin carrying, and even wearing, RFID-tagged items. At present, tens of millions of contactless credit and ATM cards containing RFID tags are in circulation, along with millions of employee access badges. RFID-based public-transit passes, widely used in Europe and Japan, are also coming to U.S. cities. IBM's person tracking unit is still only a patent, but an English amusement park called Alton Towers provides a living illustration of RFID's tracking potential. On entering the park, each visitor is offered an RFID wristband encoded with a unique ID number. As people enjoy the attractions, a network of RFID readers placed strategically throughout the park detects each wristband as it comes within range and triggers nearby video cameras. Candid footage of each individual is stored in a file labeled with the wristband ID number, then made available to the customer on a keepsake DVD at the end of the day.

Protecting the Public

If RFID tags can enable an amusement park to capture detailed, personalized videos of thousands of people a day, imagine what a determined government could do—not to mention marketers or criminals. That is why my colleagues in the privacy community and I have so firmly opposed the use of RFID in government-issued identity documents or individual consumer items. As far back as 2003, my organization, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)—along with the Privacy Rights Clearinghouse, the

Electronic Privacy Information Center, the Electronic Frontier Foundation, the American Civil Liberties Union, and 40 other leading privacy and civil liberties advocates and organizations—recognized this threat and issued a position paper that condemned the tracking of human beings with RFID as inappropriate.

In response to these concerns, dozens of U.S. states have introduced RFID consumer-protection bills—which have all been either killed or gutted by heavy opposition from lobbyists for the RFID industry. When the New Hampshire Senate voted on a bill that would have imposed tough regulations on RFID in 2006, a last-minute floor amendment replaced it with a two-year study instead. (I was appointed by the governor to serve on the resulting commission.) That same year a California bill that would have prohibited the use of RFID in government-issued documents passed both houses of the legislature, only to be vetoed by Governor Arnold Schwarzenegger.

On the federal level, no high-profile consumer-protection bills related to RFID have been passed. Instead, in 2005, the Senate Republican High Tech Task Force praised RFID applications as "exciting new technologies" with "tremendous promise for our economy" and vowed to protect RFID from regulation or legislation.

In the European Union, regulators are at least examining the situation. The European Commission—the executive arm of the E.U.—has acknowledged the potential for serious privacy problems with RFID and opened a public comment period earlier this year. As of July, when this issue went to press, recommendations stemming from the public comments were set to be released later in the summer, but expectations for any consumer-privacy regulations were low. In a March 2007 speech, E.U. commissioner for information society and media Viviane Reding announced that the commission would not regulate RFID but instead would allow businesses to regulate themselves. "I am here to tell you that on RFIDs, there is not going to be a regulation," she said. "My view is that we should underregulate rather than overregulate so that this sector can take off."

Unfortunately, industry self-regulation has little force when it comes to protecting the public from RFID risks. EPCglobal, the industry body that now sets technical standards for RFID tags, also produced a set of guidelines for the use of the chips in retail. The organization's recommendations require, among other things, notice to consumers whenever products contain RFID tags—for instance, in the form of a recognizable RFID logo. Yet when Checkpoint Systems, a member company of EPCglobal, designed RFID tags to be hidden in the soles of shoes—in clear violation of the organization's own provisions—Mike Meranda, then president of EPCglobal, told me that since the guidelines were voluntary, there was nothing he or his organization could do about it.

The Washington State Department of Licensing reassures citizens that their personal information is safe because the RFID tag in an enhanced driver's license "doesn't have a power source" and "doesn't contain any personal identifying information"—even though those facts have no bearing on whether the card can be used for tracking. For some people, a false sense of assurance provided by such official mollifications could be dangerous. The National Network to End Domestic Violence, a group that vocally opposes the use of RFID in identity documents and consumer products, has submitted legislative testimony describing how abusers could use the technology to stalk and monitor their victims.

Meanwhile the RFID train is barreling forward. Gigi Zenk, a spokesperson at Washington's licensing agency, recently confirmed that there are 10,000 enhanced licenses "on the street now—that people are actually carrying." That's a lot of potential for abuse, and it will only grow. The state recently mustered a halfhearted response, passing a law that designates the unauthorized reading of a tag "for the purpose of fraud, identity theft, or for any other illegal purpose" as a class C felony, subject to five years in prison and a $10,000 fine. Nowhere in the law does it say, however, that scanning for other purposes such as marketing—or perhaps "to control the population"—is prohibited. We ignore these risks at our peril.

Note: This article was originally published with the title, "RFID Tag--You're It".

Further Reading

Building the 21st-Century Mind
How Business Can Influence Climate Policy
Readers Respond on "A Sunshade for Planet Earth"
Remembering the Day the World Wide Web Was Born

The Future of Computing (circa 1999)
How the Mind Works (in a Cemetery)